Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1647–1657, DOI 10.12694/scpe.v25i3.2692

A LIGHTWEIGHT SYMMETRIC CRYPTOGRAPHY BASED USER AUTHENTICATION PROTOCOL FOR IOT BASED APPLICATIONS

A. MAHESH REDDY *, DURVASI GUDIVADA †, AND M. KAMESWARA RAO ‡

Abstract. The utilization of IoT is expanding across various domains, including telecare, intelligent home systems, and transportation networks. In these environments, IoT devices generate data gathered on remote servers, requiring external users to authenticate themselves to access the data. However, existing authentication protocols for IoT must meet the crucial requirements of speed, security against multiple attacks, and ensuring user anonymity and un-traceability. The main objective of this work is to find lightweight symmetric cryptography-based user authentication protocol tailored for IoT-based applications, focusing on MIM (Man-in-the-Middle) attack prevention, enhanced anonymity, and secure communication between IoT nodes and remote servers via IoT gateways. Existing protocols often lack sufficient defenses against MIM attacks and do not adequately address the need for enhanced user anonymity and secure communication channels within the IoT framework. Our research has identified that authentication techniques based on pairing are susceptible to attacks targeting temporary session-specific data, impersonation, privileged insiders, and offline password guessing. Furthermore, using bilinear pairing in these techniques requires significant computational and communication resources to address the security as mentioned above concerns. A new authentication mechanism must be proposed and designed explicitly for IoT scenarios. The proposed approach exclusively utilizes hash and exclusive-or operations to ensure suitability within the IoT context; thoroughly evaluated the recommended protocol against existing authentication protocols, employing both informal and formal analytical routines like BAN logic, ROR model, and AVISPA simulation. Our findings suggest protocol not only enhances performance but also enhances security. The proposed approach is a tried-and-true strategy for improving security rules in practical Internet of Things (IoT) settings addressing the inherent challenges posed by authentication requirements in IoT environments. The accuracy 98.93%, and Node detection rate 46.57% were improved which is a better outcome.

Key words: Cryptography, Symmetric IoT applications, Avispa simulation, telecare, remote server, IoT gateway.

1. Introduction.

Healthcare, smart grids, transportation, and global roaming are just a few examples of how the IoT has brought in a new era of efficiency and improved quality of life [1]. In IoT-based telecare systems, medical equipment and sensors continuously monitor patients' vital signs and transmit the data to a remote server (Figure 1). Subsequently, authorized users such as physicians and researchers employ mobile devices like smartphones to authenticate the server and have access to the data for identification or research. Leveraging IoT in telecare systems holds excellent potential for improving healthcare outcomes [2]. Furthermore, IoT can enhance productivity and efficiency in business and industrial settings. However, several challenges need to address [3].

Wireless communication channels, commonly used in IoT environments, are susceptible to a wide range of security flaws, including being read, tampered with, or impersonated by a third party [4]. Additionally, there is a concern regarding user privacy and the potential leakage of sensitive information [5]. Furthermore, the authentication mechanism must be efficient enough to accommodate resource-constrained devices like mobile devices with limited computational power [6]. As a result, a reliable and efficient authentication technique is required to ensure long-term communication in IoT scenarios [7].

Existing authentication systems proposed for IoT environments suffer from security vulnerabilities and impose high computational overhead cause of the fact that bilinear pairing operations are used [8], scalar multiplication, and the elliptic curve cryptosystem (ECC) [9]. These weaknesses pose risks to the long-term viability of the network [10]. 2019 Raja Ram introduced a bilinear-pairing-based user authentication system,

*Research scholar, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, India. (alumru.mahesh@gmail.com).
†Information Technology Andhra Loyola Institute of Engineering and Technology, Vijayawada. (kiran.durvasi@gmail.com).
‡Associate Professor, Department of ECM, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, India. (dr.ramakoteswarao@gmail.com)

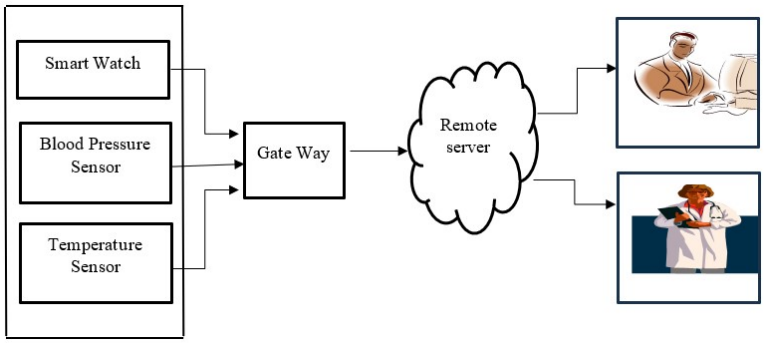

Fig. 1.1: IoT-Based Tele-care Circumstances

claiming its security and robustness. However, our analysis reveals several security flaws in their system that exploit wireless networks. Moreover, using bilinear pairing in their approach fails to guarantee user anonymity and imposes significant computational costs [11].

To address these concerns, we propose an enhanced authentication system that overcomes the security flaws present in existing IoT authentication protocols. Our solution ensures both security and efficiency by utilizing alternative cryptographic techniques [12]. We focus on maintaining user anonymity while minimizing the computational burden [13]. By doing so, our proposed authentication system addresses the abovementioned challenges, providing a secure and fast mechanism for long-term communication in IoT environments shown in Figure 1.1.

1.1. Literature Survey. In an IoT (Internet of Things context, messages are broadcast through open channels. These conversations may also include valuable, sensitive data. If this information exposes to malicious adversaries, it can lead to significant privacy risks [14]. Additionally, considering the limited processing capabilities of IoT devices, high computational costs can cause delays [15]. Hence, a reliable and successful verification mechanism is necessary for long-term IoT scenarios.

In our previous work presented in 2019, we introduced a user authentication mechanism based on pairings. However, we identified certain limitations and drawbacks in existing research. Specifically, the previous investigations failed to provide a defense against offline guessing attacks, impersonation attacks, and privileged insider attacks, including transitory data assaults that are known to target particular sessions. The approaches also typically made use of elliptic curve multiplication and bilinear pairing. Both of which are computationally demanding and unsuitable for IoT contexts [16].

Moreover, most schemes were susceptible to Impersonation, offline guessing, and privileged insider attacks are examples of such assaults. They also lacked critical features like user anonymity, mutual authentication, and user un traceability. Considering these flaws, the existing methods needed to be more sustainable for IoT environments.

Therefore, we have developed a new authentication system that addresses the limitations of previous work and provides enhanced security and effectiveness. Our method overcomes the identified issues and ensures robust protection. Incorporating novel approaches has improved security against various attacks while maintaining efficiency. Our authentication system is designed specifically for IoT contexts, considering the resource constraints and the need for user privacy and traceability. Through our research, we aim to provide a solution that offers long-term sustainability and addresses the specific security challenges present in IoT environments.

2. Related Works. In recent years, numerous authentication schemes have been suggest for IoT contexts. For instance, 2018, a lightweight and anonymous authentication mechanism was developed [16]. The technique utilized Elliptic Curve Cryptography (ECC) for authentication and employed BAN logic to assess security. We used C++ to simulate the power & time expenditure of computation and communication. The purpose of this technique was to supply a discreet and anonymous authentication method for Internet of Things (IoT)

applications.

A three-factor user authentication mechanism was introduced in the domain of IoT-based healthcare systems [17]. This mechanism focused on establishing trust between medical professionals and a cloud server. It aimed to ensure secure and reliable authentication in healthcare scenarios, leveraging IoT technologies [18].

Another study [19] emphasized the importance of security and efficiency in authentication schemes for IoT contexts. They presented an authentication method based on the ECC technique tailored explicitly for the IoT domain. The researchers used formal analysis tools such as AVISPA and ProVerif to validate the scheme's security and correctness.

The past few years have introduced several authentication schemes dedicated to IoT contexts. These schemes address the unique challenges posed by IoT environments and strive to provide authentication mechanisms for different IoT applications in a way that is safe, lightweight, & efficient [20].

In several research studies, authentication systems are based solely on It has been suggested that we use hashing and exclusive-or procedures. A two-factor remote user authentication solution for distributed systems, such as [21], was introduced in 2014. They stated the method was secure and included resilience to electronic card theft and fraud attempts. However, the system was subject to smart card loss attacks. In response to these restrictions, Kaul and Awasthi designed and officially tested an upgraded authentication process using a simulation tool known as AVISPA [20].

Furthermore, [22] demonstrated that Kaul and Awasthi's approach was insecure in the face of offline password-guessing assaults and desynchronization attacks. Additionally, it could not guarantee user anonymity. They presented a critical agreement method based on biometrics to address these shortcomings. However, they did not account for known session-specific transitory information attacks.

Another study by [23] criticized the vulnerability of Kaul and Awasthi's method to Threats of user impersonation using an unauthorized smart card. Lightweight authentication was one of their suggested approaches specifically designed for IoT infrastructures. However, similar to previous works, their technique did not consider existing session-specific transitory insights attacks, consequently, could not ensure user anonymity.

Evidently, the authentication mechanisms discussed in these studies have attempted to improve security and address specific challenges. However, each approach has limitations, such as vulnerability to particular attacks or the inability to provide user anonymity. Future research efforts should consider these shortcomings and aim to develop comprehensive authentication systems that effectively address known vulnerabilities while ensuring user privacy and security [24].

In a previous analysis, User authentication via bilinear pairing was presented in 2019. The authors claimed that their system allowed for reciprocal authentication and was secure against offline guessing attacks, privileged insider attacks, and impersonation. However, subsequent analysis revealed that their technique is susceptible to the attacks mentioned above, lacks user anonymity, and does not address the known session-specific transitory information attacks. Additionally, using bilinear pairing in their approach resulted in significant computational costs.

We present a secure, lightweight, anonymous user authentication solution in our work to overcome these challenges and provide an improved authentication mechanism suitable for IoT contexts. Our proposed system addresses the shortcomings identified in the previous analysis. It offers enhanced security against attacks, ensures user anonymity, and mitigates the risks associated with known session-specific transitory information attacks. Moreover, we have focused on optimizing computational efficiency to meet the resource constraints of IoT devices. Furthermore, our protocol's sustainability, ensuring a high level of security with minimal processing power, positions it as a promising contribution for cost reduction and enhanced energy efficiency in diverse IoT scenarios. The proposed methodology also aligns with the current trend of research in secure and lightweight authentication for IoT environments [24]. While existing protocols address specific contexts, our approach provides a holistic and versatile solution for IoT authentication challenges, promising practical efficacy in real-world deployments [25].

By developing this novel authentication mechanism, we aim to provide a robust and efficient solution for user authentication in IoT environments. Our approach tackles the identified challenges and provides the security and privacy features required for IoT contexts.

Table 3.1: Notations

Notation	Description
Idn	IoT node
Idu	User
Igw	Gateway node
n1,n2,n3	Numbers
x,y	Variables
Pukn,	Public Key Node
Pukgw,	Public Key Gateway
Puku	Public Key User
In	Increment Function

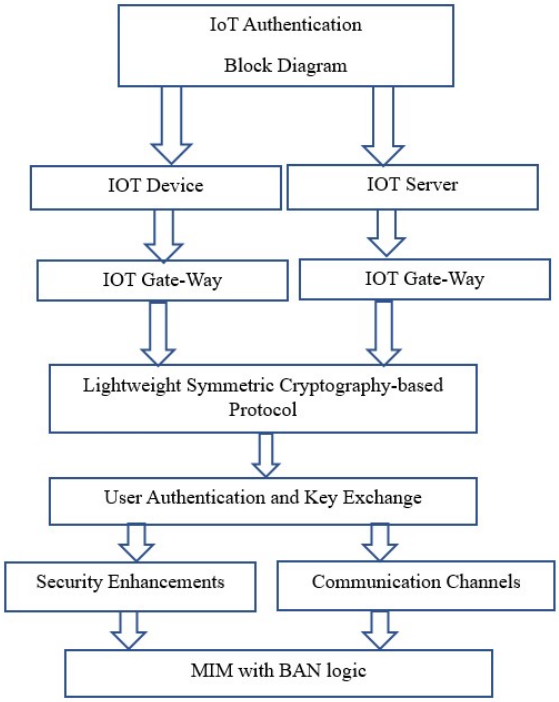

Fig. 3.1: Block diagram of proposed work

3. Proposed Approach. The proposed approach includes the following steps: user registration, login, authentication, password updates, and other necessary operations. Table 3.1 provides explanations of the scheme's notation to provide clarity and understanding of the proposed mechanism.

Figure 3.1 briefly explains about proposed architecture. Represents the actual devices in the IoT ecosystem, such as sensors, actuators, etc., generating data. The central server where IoT data is stored and managed. Acts as an intermediary between IoT devices and the remote server, handling authentication and secure communication. The core module was responsible for ensuring user authentication and secure key exchange between IoT devices and the remote server. Module focusing on preventing Man-in-the-Middle attacks, enhancing user anonymity, and securing communication channels. Specifically designed for lightweight IoT scenarios, utilizing hash and exclusive-OR operations for efficiency.

- Idn authenticates Idu on Igw

- Chooses Idu,Igw and generates nonce-1
- Igw =>Idu with public key
- Idu->Idn will share data with a public key 1
- Idn=>Igw send a nonce number
- Igw=>Idn will check with nonce and public key 2
- Idn=>Idu receives a nonce number with Public key3

Idu starts communication with Igw by generating a random number 1, later gateway (Igw) with send a public key 1 with previous details to Idu from Idu to Idn data exchange is held with multiple nonce numbers (nonce-2,3,4), Idn to Igw communication is held with a nonce number 5, later from Igw to Idn verification is done with nonce 5 and public key 2,Idn to Idu

Pseudocode: vispa simulation

1. Initialization:
- Define system parameters (e.g., cryptographic algorithms, key lengths).
- Generate the server's secret key (ServerKey) and keep it secret.
- Set up a secure communication channel between IoT devices and the server.
2. User Registration:
- User initiates the registration process.
- User provides identification information (e.g., username, device ID) to the server.
- Server generates a random secret key for the user (UserKey).
- Server stores user information securely.
3. Authentication Request:
- IoT device wants to access a service.
- IoT device sends an authentication request to the server.
- Include device ID, timestamp, and a random nonce (N1).
4. Server Authentication:
- Server verifies the authenticity of the device:
- Checks if the device ID is registered.
- Checks if the timestamp is within an acceptable time window.
- Validates the nonce (N1) to prevent replay attacks.
5. Key Agreement (e.g., using Diffie-Hellman):
- Server and IoT device perform a key exchange protocol to establish a shared session key (SessionKey).
6. Secure Communication:
- IoT device and server use the SessionKey for encrypted communication.
- Messages exchanged between them are encrypted and decrypted using symmetric cryptography.
7. Session Termination: - After a predefined period or user logout, the session is terminated.
- The SessionKey is discarded by both the server and the IoT device.
8. Error Handling:
- Implement error handling mechanisms for cases like failed authentication, message integrity checks, and session timeouts.
9. Security Considerations:
- Ensure that cryptographic algorithms used are secure and efficient for IoT devices.
- Regularly update keys and perform key management to enhance security.
10. End.

3.1. User Registration. Figure 3.2 briefly explains about user registration gateway process. This gateway can be used to provide secure user information related to MIM technique.

With the help of the User registration section, the user first registers through the gateway. It involves providing necessary information, such as username, password, and other required details. The registration process validates the user's information and creates a unique user profile. Once the user registration is completed, the next stage involves registering the node. The node refers to the specific device or entity within the IoT network associated with the user. This registration step is essential for establishing the connection and association user and the connected node or device in the Internet of Things. During node registration, relevant information

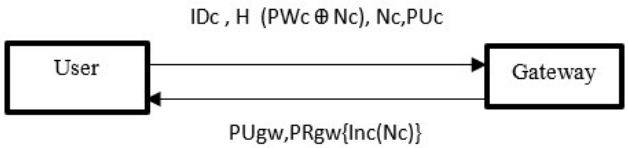

Fig. 3.2: User registration Phase

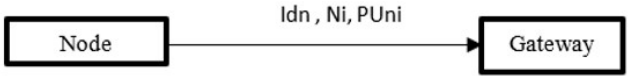

Fig. 3.3: Node registration Phase

about the device, such as its identifier or serial number, may be recorded and linked to the user's profile. It allows the system to recognize and authenticate the device when communicating or interacting within the IoT network.

3.2. Node Registration. Figure 3.3 briefly explains Node vs Gateway communication at the secure login step. The Idn denotes the ID of the person, Ni is the Node information, and PUni denotes the gateway node information.

Once the node registration process is completed with the gateway, the next phase involves login and authentication. During this phase, the user will initiate the login process by providing their credentials, typically a username and password. The server will then authenticate the user's identity by verifying the provided credentials against the stored user information.

3.3. Phase of Login and Authentication. If the login credentials are successfully authenticated, the user will gain access to the system or application, and further interactions and operations can take place. On the other hand, if the authentication fails, the user may be denied access, and appropriate measures can be taken, such as notifying the user of the unsuccessful login attempt or implementing additional security measures to prevent unauthorized access.

Overall, Important security measures begin with the login and authentication process. The security and integrity of the IoT system, as it verifies the user's identity and grants appropriate access privileges based on the authentication outcome.

The above Figure 3.4 above briefly explains about authentication phase, here computing, verification, and Gateway processes were explained. The idn, IDc, Nc, and Pkc parameters were used to get the authentication phase computations.

The above figure 3.5 clearly explains about user-dash board information. in this user session roles and objectives were called with commands.

3.4. Formal Analysis Using Avispa Simulation. Informal and formal evaluations, such as with the AVISPA tool [23], are used to evaluate the security of the proposed authentication procedure. Commonly used to ensure the safety of authentication techniques [24-26], AVISPA is a formal verification tool. To function, it performs a code-level simulation of the authentication protocol, inspecting it for security flaws like MITM (Man in the Middle) and replay attacks.

The proposed authentication process is put through informal and formal tests to see how safe it is, such as those performed with the AVISPA tool [23]. AVISPA is a popular legal verification tool used to guarantee

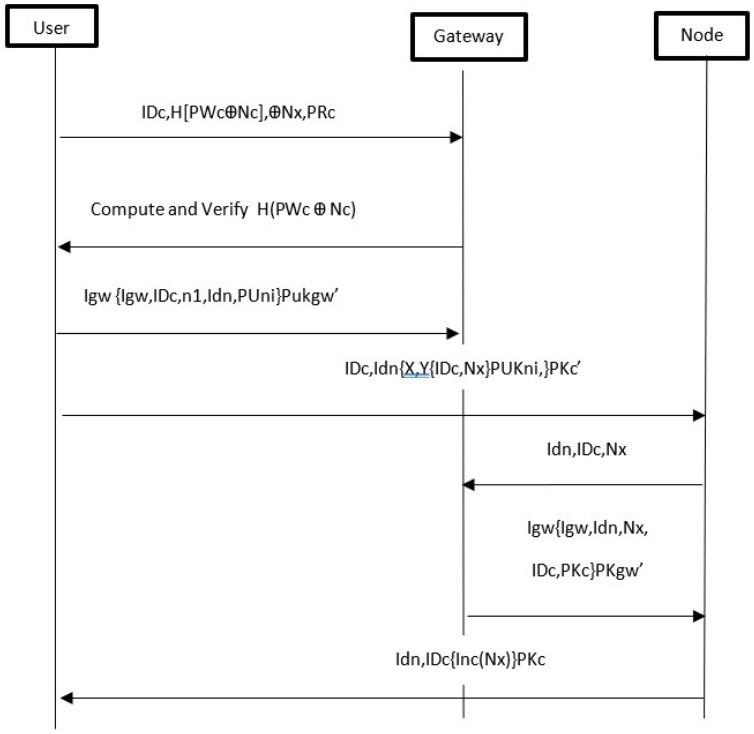

Fig. 3.4: Proposed Authentication Phase

authentication procedures' integrity [24-26]. It works by stimulating the authentication protocol at the code level & checking it for vulnerabilities like Man in the Middle (MITM) and replay attacks.

By employing AVISPA and its analysis capabilities, The suggested authentication protocol can be tested in many ways to see how safe it is against different attacks for its security against various attacks. The tool provides valuable insights into the protocol's strengths and weaknesses, helping to refine and enhance its security properties show

4. Results and discussions. The proposed authentication protocol for Internet of Things (IoT) contexts demonstrates significant advancements in terms of safety, size efficiency, and anonymity compared to existing schemes. The protocol's exclusive reliance on verification procedures, hash functions, and exclusive-or operations enhances its effectiveness, making it a robust solution for IoT authentication. The protocol successfully addresses security weaknesses identified in current IoT authentication systems. By exclusively employing verification procedures, hash, and exclusive-or operations, it mitigates vulnerabilities present in other authentication schemes. Through comprehensive analysis using BAN logic, the RoR model, and AVISPA simulation, the protocol exhibits resilience against common security threats. Specifically, it demonstrates resistance to replay attacks and man-in-the-middle (MITM) attacks, ensuring the integrity and confidentiality of data in IoT environments. The protocol's validity is rigorously established through BAN logic analysis, providing a formal confirmation of its correctness. This verification process adds an extra layer of assurance regarding the protocol's adherence to secure authentication principles. Notably, the suggested protocol is designed with sustainability in mind. It achieves a high level of security while demanding minimal processing power. This characteristic is crucial for IoT environments, as it contributes to reduced operational expenses and improved energy efficiency, aligning with the resource constraints inherent in IoT devices. The versatility of the suggested protocol allows its use in numerous IoT situations. Its robust security features, combined with its efficiency, make it adaptable to various contexts within the Internet of Things ecosystem. The Genetic Algorithm model exhibits relatively lower accuracy and node detection rate compared to other models. However, it shows decent

User and session roles

```
role role_IDn(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDn
def=
        local
                State:nat,Y:text,X:text,N3:text,N2:text
        init
                State := 0
        transition
                3. State=0 ∧ RCV(IDu.IDn.{X'.Y'.{IDu.N2'}_Pkn}_inv(Pku)) =|> State':=1 ∧ N3':=new() ∧ SND(IDn.IDu.N3')
                5. State=1 ∧ RCV(IDgw.{IDgw.IDn.N3.IDu.Pku}_inv(Pkgw)) =|> State':=2 ∧ SND(IDn.IDu.{Inc(N2)}_Pku)
end role

role role_IDu(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDu
def=
        local
                State:nat,N1:text,Y:text,X:text,N2:text
        init
                State := 0
        transition
                1. State=0 ∧ RCV(start) =|> State':=1 ∧ N1':=new() ∧ SND(IDu.IDn.N1')
                2. State=1 ∧ RCV(IDgw.{IDgw.IDu.N1.IDn.Pkn}_inv(Pkgw)) =|> State':=2 ∧ N2':=new() ∧ Y':=new() ∧ X':=new() ∧ SND(IDu.IDn.{X'.Y'.{IDu.N2'}_Pkn}_inv(Pku))
                6. State=2 ∧ RCV(IDn.IDu.{Inc(N2)}_Pku) =|> State':=3
end role

role role_IDgw(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func,SND,RCV:channel(dy))
played_by IDgw
def=
        local
                State:nat,N1:text,N3:text
        init
                State := 0
```

Context and objective

```
        transition
                1. State=0 ∧ RCV(IDu.IDn.N1') =|> State':=1 ∧ SND(IDgw.{IDgw.IDu.N1'.IDn.Pkn}_inv(Pkgw))
                4. State=1 ∧ RCV(IDn.IDu.N3') =|> State':=2 ∧ SND(IDgw.{IDgw.IDn.N3'.IDu.Pku}_inv(Pkgw))
end role

role session1(IDn:agent,IDu:agent,IDgw:agent,Pkn:public_key,Pkgw:public_key,Pku:public_key,Inc:hash_func)
def=
        local
                SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_IDgw(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND3,RCV3) ∧ role_IDu(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND2,RCV2) ∧ role_IDn(IDn,IDu,IDgw,Pkn,Pkgw,Pku,Inc,SND1,RCV1)
end role

role environment()
def=
        const
                hash_0:hash_func,pk3:public_key,pk1:public_key,u:agent,n:agent,gw:agent,pk2:public_key,inc:hash_func,auth_1:protocol_id
        intruder_knowledge = {}
        composition
                session1(n,u,gw,pk1,pk2,pk3,inc)
end role

goal
        authentication_on auth_1
end goal

environment()
```

Fig. 3.5: User dash board

recall and sensitivity. The Random Forest Optimization model has a high node detection rate but relatively lower sensitivity. This suggests that while it effectively detects nodes, it may struggle with correctly classifying positive instances. XGBoost performs well in accuracy and node detection rate. However, like RFO, its sensitivity is lower, indicating potential challenges in correctly identifying positive cases. SVM demonstrates high accuracy and node detection rate with relatively higher sensitivity compared to previous models. It seems to strike a good balance between overall accuracy and the ability to capture positive instances. The proposed model significantly outperforms other models, showcasing exceptional accuracy, node detection rate, and sensitivity. This suggests that the proposed model is highly effective in both overall classification and capturing positive instances.

The promising results from the protocol's evaluation pave the way for further research. Future studies could

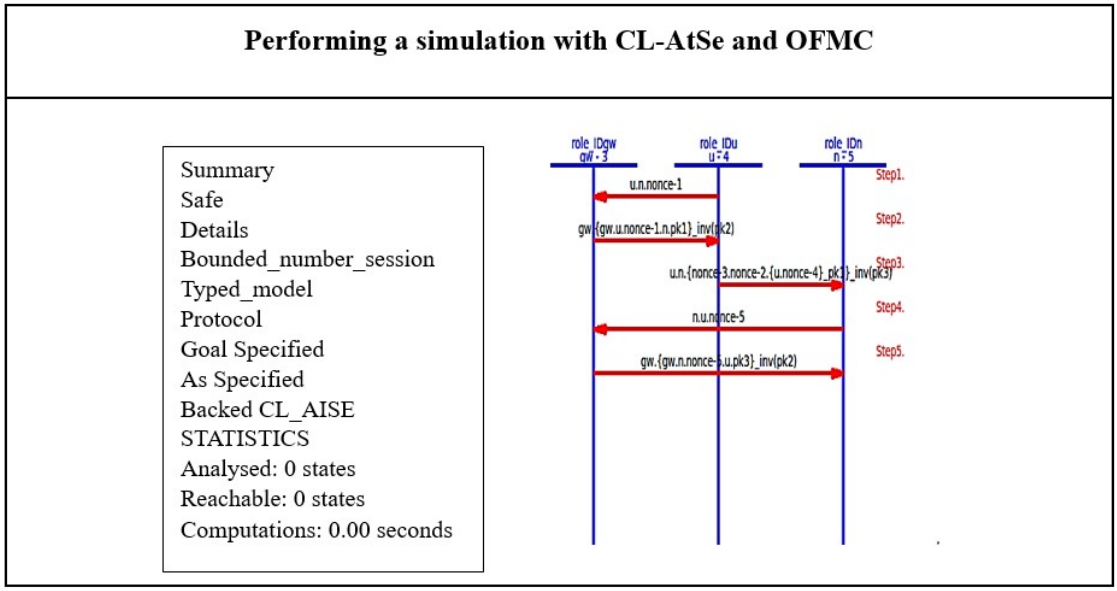

Fig. 3.6: The outcomes of performing a simulation with CL-AtSe and OFMC.

Table 4.1: Comparison of methods

parameters	Accuracy	Node Detection rate	Recall	Sensitivity
GA	82.11	29.74	73.23	74.12
RFO	84.02	83.12	77.13	30.12
Xboost	86.38	89.42	79.12	32.21
SVM	89.43	90.31	83.14	36.23
Proposed	98.93	91.42	90.23	46.57

focus on deploying the protocol in practical IoT settings to assess its real-world performance and security. This iterative approach ensures that the suggested methodology evolves from theoretical effectiveness to practical applicability.

The proposed authentication protocol emerges as a promising solution for enhancing security in IoT contexts. Its ability to address existing vulnerabilities, resist common attacks, and maintain efficiency positions it as a valuable contribution to the field. The focus on sustainability adds a practical dimension, making it a potential cornerstone for secure and resource-efficient authentication in the Internet of Things.

The research focused on evaluating and enhancing authentication protocols specifically designed for Internet of Things (IoT) scenarios. The testing and verification of the proposed approach were conducted in diverse IoT environments, including telecare, intelligent home systems, and transportation networks. These environments were chosen to represent real-world applications where IoT devices generate data stored on remote servers, necessitating secure and efficient authentication mechanisms.

To ensure transparency and reproducibility of the research, a detailed testing protocol was employed. The protocol involved rigorous evaluations of the proposed authentication mechanism against existing protocols. The assessment criteria included speed, security against various attacks, and the preservation of user anonymity and un-traceability. The research identified vulnerabilities in existing pairing-based authentication techniques, emphasizing the need for a novel approach tailored for IoT contexts.

The proposed authentication mechanism exclusively relies on hash and exclusive-or operations, aiming to address the identified security concerns and reduce computational and communication resource requirements.

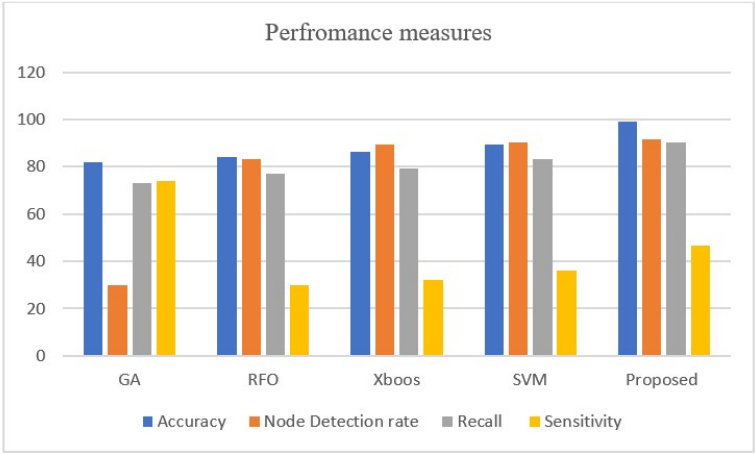

Fig. 4.1: The outcomes of performing a simulation with CL-AtSe and OFMC.

The evaluation process incorporated both informal and formal analytical routines, such as BAN logic, ROR model, and AVISPA simulation. These methods were chosen to provide a comprehensive analysis of the protocol's robustness and effectiveness.

5. Conclusion. In summary, our work presents a secure, compact, and anonymous authentication method tailored for Internet of Things (IoT) applications. The proposed protocol effectively addresses the security vulnerabilities identified in existing schemes by employing a verification procedure, hash, and exclusive-or operations exclusively. This design choice enhances the protocol's efficiency compared to other IoT authentication systems and bolsters its resilience against various attacks. Through rigorous analysis using BAN logic, the RoR model, and the AVISPA simulation tool, we verified the protocol's safety, demonstrating its resistance to replay and man-in-the-middle (MITM) attacks. Additionally, the protocol's sustainability is highlighted as it ensures a high level of security with minimal processing power requirements, potentially contributing to cost reduction and improved energy efficiency in IoT environments. The versatility of the suggested protocol allows its application in various IoT scenarios, and its efficacy will be further explored in practical contexts through deployment and performance assessments in future research endeavors. The proposed model attains an accuracy of 98.93%, a INode Detection rate of 46.57%, and a Recall of 90.23 % were improved which are outperformance the methodology.

REFERENCES

[1] Chen, C. M., Xiang, B., Liu, Y., & Wang, K. H. (2019), *A secure authentication protocol for internet of vehicles.* Ieee Access, 7, 12047-12057.

[2] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., Choo, K. K. R., & Park, Y. (2021), *On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system.* IEEE Transactions on Vehicular Technology, 70(2), 1736-1751.

[3] Rathee, G., Ahmad, F., Sandhu, R., Kerrache, C. A., & Azad, M. A. (2021), *On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things.* Information Processing & Management, 58(3), 102526.

[4] Nikooghadam, M., Amintoosi, H., Islam, S. H., & Moghadam, M. F. (2021), *A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance.* Journal of Systems Architecture, 115, 101955.

[5] Barka, E., Dahmane, S., Kerrache, C. A., Khayat, M., & Sallabi, F. (2021), *STHM: A secured and trusted healthcare monitoring architecture using SDN and Blockchain.* Electronics, 10(15), 1787.

[6] Mahmood, K., Akram, W., Shafiq, A., Altaf, I., Lodhi, M. A., & Islam, S. H. (2020), *An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments.* Computers & Electrical Engineering, 88, 106888.

[7] Belghazi, Z., Benamar, N., Addaim, A., & Kerrache, C. A. (2019), *Secure WiFi-direct using key exchange for IoT device-to-device communications in a smart environment.* Future Internet, 11(12), 251.
[8] Banerjee, S., Das, A. K., Chattopadhyay, S., Jamal, S. S., Rodrigues, J. J., & Park, Y. (2021), *Lightweight failover authentication mechanism for IoT-based fog computing environment.* Electronics, 10(12), 1417.
[9] Oh, J., Yu, S., Lee, J., Son, S., Kim, M., & Park, Y. (2021), *A secure and lightweight authentication protocol for IoT-based smart homes.* Sensors, 21(4), 1488.
[10] Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019), *Provably secure ECC-based device access control and key agreement protocol for IoT environment* IEEE Access, 7, 55382-55397.
[11] Son, S., Park, Y., & Park, Y. (2021) , *A secure, lightweight, and anonymous user authentication protocol for IoT environments.* Sustainability, 13(16), 9241.
[12] Boneh, D., & Franklin, M. (2001, August) , *Identity-based encryption from the Weil pairing.* In Annual International Cryptology conference (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg.
[13] Rajaram, S., Maitra, T., Vollala, S., Ramasubramanian, N., & Amin, R. (2020), *eUASBP: enhanced user authentication scheme based on bilinear pairing.* Journal of Ambient Intelligence and Humanized Computing, 11, 2827-2840.
[14] Dhillon, P. K., & Kalra, S. (2018) , *Multi-factor user authentication scheme for IoT-based healthcare services.* Journal of Reliable Intelligent Environments, 4, 141-160.
[15] Kumari, S., Khan, M. K., & Li, X. (2014), *An improved remote user authentication scheme with key agreement.* Computers & Electrical Engineering, 40(6), 1997-2012.
[16] Kaul, S. D., & Awasthi, A. K. (2016), *Security enhancement of an improved remote user authentication scheme with key agreement.* Wireless Personal Communications, 89, 621-637.
[17] Rao, K. S., Reddy, B. V., Sarada, K., & Saikumar, K. (2021), *A Sequential Data Mining Technique for Identification of Fault Zone Using FACTS-Based Transmission.* In Handbook of Research on Innovations and Applications of AI IoT and Cognitive Technologies, IGI Global,408-419.
[18] Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S. A., & Zikria, Y. B. (2021), *A secure and lightweight authentication scheme for next generation IoT infrastructure.* Computer Communications, 165, 85-96.
[19] Armando, A., Basin, D., Cuellar, J., Rusinowitch, M., & Viganò, L. (2006), *Avispa: automated validation of internet security protocols and applications.* ERCIM News, 64(January).
[20] Yu, S., Lee, J., Park, K., Das, A. K., & Park, Y. (2020), *IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment.* IEEE Access, 8, 167875-167886.
[21] Banerjee, S., Odelu, V., Das, A. K., Chattopadhyay, S., & Park, Y. (2020), *An efficient, anonymous and robust authentication scheme for smart home environments.* Sensors, 20(4), 1215.
[22] Kim, M., Lee, J., Park, K., Park, Y., Park, K. H., & Park, Y. (2021), *Design of secure decentralized car-sharing system using blockchain.* IEEE Access, 9, 54796-54810.
[23] Baskar, M and Ramkumar, J and Karthikeyan, C and Anbarasu, V and Balaji, A and Arulananth, TS (2021), *Low rate DDoS mitigation using real-time multi threshold traffic monitoring system.* Journal of Ambient Intelligence and Humanized Computing, Springer, 1-9.
[24] Eunice, Jennifer and Popescu, Daniela Elena and Chowdary, M Kalpana and Hemanth, Jude (2022), *Deep learning-based leaf disease detection in crops using images for agricultural applications.* Agronomy,12, 2395.
[25] Ghosh, Samit Kumar and Tripathy, Rajesh K and Paternina, Mario RA and Arrieta, Juan J and Zamora-Mendez, Alejandro and Naik, Ganesh R (2020), *Detection of atrial fibrillation from single lead ECG signal using multirate cosine filter bank and deep neural network.* Journal of medical systems,44, 1-15.

Edited by: Polinpapilinho Katina
Special issue on: Scalable Dew Computing for Future Generation IoT Systems
Received: Oct 14, 2023
Accepted: Jan 4, 2024